UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,547	06/06/2000	TARO TERAO	106408	8229

25944 7590 02/13/2004

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	4

DATE MAILED: 02/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/588,547	**Applicant(s)** TERAO, TARO	
	Examiner Jung W Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *38* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 June 2000* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-38 have been examined.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 16 (see page 34). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "T", "36", and no reference have been used to designate a proving instrument. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

4. The disclosure is objected to because of the following informalities: on page 23, the specification lists the hash value calculation unit as Reference No. 6; it should be identified as Reference No. 5 as listed in the drawings. Appropriate correction is required.

Claim Objections

5. Claims 19 and 32 are objected to because of the following informalities: claim 19 is poorly worded; in claim 32, the bit concatenation "(u1 | M) | ... | H(um |)" should be "H(u1 | M) | ... | H(um | M)" based on applicant's disclosure on page 20. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 5, 7, 25, 28, and 33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. When using means plus function language in a claim, the applicant is required in the specification to provide adequate disclosure to support the limitations indicated in the claim. The proper test for meeting the definiteness requirement is that the corresponding structure of a means-plus-function limitation must be disclosed in the specification itself in a way that one skilled in the art will perform the recited function. See MPEP § 2181-217. The following structure(s) do not meet the definiteness requirement: claims 5, 7, 24, 25, 28, and 33 specify means for creating a one-way function value X(M); however, the specification does not clearly define means to perform the creation step.

8. Claim 28 recites the limitation "the private key x". There is insufficient antecedent basis for this limitation in the claim.

9. Claim 7, 13, 20-21, and 24-26 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: In regards to claims 7, 20-21, and 24-26, the relationship between the one-way function value X(M) and the private key X(M). In regards to claims 13, the relationship between the calculated commitment w and the proving device.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1,2, 5-10, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang U.S. Patent No. 6,154,541 (hereinafter Zhang) in view of Friedman et al. U.S. Patent No. 6,240,513 (hereinafter Friedman). As per claim 1, Zhang covers a method for generating a one-way-function value by applying a one-way-function to a plurality of seed values to create a hash value. These seed values and the

resulting hash value cover the values u, M, and X(M) as defined by applicant's claim 1 (see Zhang, col. 22, lines 37-46). Although Zhang does not explicitly define combining a unique value d and a unique value s to create the unique value u, Zhang does teach strategies of combining a plurality of parameters to generate new parameters using the following methods as disclosed in col. 21, line 65-col. 22, line 36 to ensure a more secure key generation methodology:

a. Segmented sequences

b. Reassembling of fragmented/fractured numbers

c. Multi-seeding

d. Reseeding

e. Any combinations of the above 4

Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to create a unique value u from the values s and d. Motivation for such a combination would hinder disclosure of the generated keys by attempts to surreptitiously analyze the key generator as taught by Zhang. Finally, Zhang does not expressly disclose the unique value s to be held by the method; however, parameter values held by a method and used as seeds for key generation is a common feature in the art. These local values, which identify a particular user or device, such as MAC, Internet address, device serial number, user identifier, etc. are typically combined with other variables to create keys. These local seed values establish a dependency of the key to the held seed value, and hence to the user or device creating the key. As an example, Friedman discloses a key generation method wherein the seed for the method is a locally held seed (see Friedman, col. 5, lines 38-44). It would be obvious to one of ordinary skill in the art at the time the invention was made for the unique value s to be stored locally. Motivation for such an implementation would establish a dependency of the key to the locally held value s as taught by Friedman. The aforementioned cover claim 1.

12. As per claim 2, Zhang covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Zhang discloses means wherein the value generation unique value u is calculated by applying a one-way function G to the function generation unique value s and the unique value d (see Zhang, col. 22, lines 31-36).

13. As per claims 5 and 6, Zhang covers a device for generating one-way function values that calculates a one-way function X dependent on a unique value d as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). In addition, Zhang teaches that the steps defined above can be implemented in a smart card (see Zhang, col. 6, line 27; col. 13, line 3). The aforementioned cover claims 5 and 6.

14. As per claims 7-9, Zhang covers a proving device for performing processing based on a private key dependent on a message M (see col. 6, lines 19-40, especially line 25) as outlined above in the claim 6 rejection under 35 U.S.C. 103(a). In addition, the device covers means for performing processing based on the private key X(M) (see Zhang, Figure 2, 'Crypt Unit B', and related text). The aforementioned cover claims 7-9.

15. As per claim 10, Zhang covers a proving device as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). Zhang does not expressly disclose that the proving device is configured as a module inside a CPU of the device. Examiner takes Official Notice that proving devices, especially those using private keys in a cryptosystem, are conventionally configured as a module inside a CPU of a device. It would be obvious to one of ordinary skill in the art at the time the invention was made to configure the proving device as a module inside a CPU of the device. Motivation for such an implementation enables the proving device to be implemented using a processor.

16. As per claim 19, Zhang covers a proving device as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, Zhang teaches that parameters defined by the method can be specified as variables controlling both the system and the keys generated (see Zhang, col. 16, lines 44-45).

17. As per claim 20, it is an apparatus claim corresponding to claim 19 and it does not teach or define above the information claimed in claim 19. Therefore, claim 20 is rejected under Zhang in view of Friedman for the same reasons set forth in the rejections of claim 19.

18. Claims 18, 21-30, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang in view of Friedman, and further in view of Stallings

Cryptography and Network Security 2nd Edition (hereinafter Stallings). As per claim 18, Zhang covers a proving device as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). Zhang is silent on the message M including use conditions of the message by the method. However, use conditions specified by a controlling message have been implemented in the analogous art of certificates. In particular, X.509 certificates define use conditions in the extensions to the standard parameters on the information established in the certificate (see Stallings, page 348, bullet 'Key usage'). As such, use conditions specifying the policies under which the values can be used or processed would be obvious to one of ordinary skill in the art at the time the invention was made. Motivation for such an implementation would enable a flexible means to distribute a plurality of types of messages and ensure that values distributed are properly processed or used.

19. As per claim 21, Zhang covers a proving device as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). Furthermore, the invention disclosed by Zhang is identified as being applicable to authentication schemes (see Zhang, col. 6, lines 19-40), which embodiments invariable cover certification authentication schemes. As taught by Stallings, certification authentication using public key encryption as listed in claim 21 is a close variant of a well-known authentication method (see Stallings, page 186, 'Public-key Certificates'). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the device disclosed by Zhang as an authentication scheme by which the device is a right issuer by means of establishing

and issuing certificates to right recipients as taught by Stallings. Motivation for such an implementation would enable an authentication device based on standard certificate authentication means.

20. As per claims 22 and 23, Zhang covers an authentication method as outlined above in the claim 21 rejection under 35 U.S.C. 103(a). In addition, an identifier aid indicating an authentication type and use conditions are included in the certification (see Stallings, Figure 11.3, 'Signature'; page 348, 'Key and Policy Information').

21. As per claims 24 and 25, they are apparatus claims corresponding to claim 21 and they do not teach or define above the information claimed in claim 21. Therefore, claims 24 and 25 are rejected under Zhang in view of Friedman and Stallings for the same reasons set forth in the rejection of claim 21.

22. As per claims 26 and 27, Zhang covers an authentication method as outlined above in the claim 22 rejection under 35 U.S.C. 103(a). In addition, the access ticket specified in the applicant's claims 26 and 27 is equivalent to the issued certificate generated by the right issuer and issued to the right recipient whereupon the rights of the right recipient is verified by means of the certificate as claimed in claim 22. Hence, claims 26 and 27 are covered by the invention covered by Zhang and Friedman modified by Stallings.

23. As per claim 28, it is an apparatus claim corresponding to claim 26 and it does not teach or define above the information claimed in claim 26. Therefore, claim 28 is rejected under Zhang in view of Friedman and Stallings for the same reasons set forth in the rejection of claim 26.

24. As per claims 29 and 30, Zhang covers an access ticket issuing device as outlined in the claim 28 rejection under 35 U.S.C. 103(a). Zhang does not expressly disclose the access ticket being calculated as a difference between the private key x and the generated private key X(M) nor as a quotient x/X(M). However, as known in the art, the difference or quotient of two values are typical mathematical operations to divine the equality of the two values: the difference of two equal values is zero whereas the quotient of two equal, nonzero values is one. It would be obvious to one of ordinary skill in the art at the time the invention was made to calculate the access ticket as being calculated as the difference or quotient of the values x and X(M). Motivation for such an implementation allows for a simple calculation to determine if a generated value is equivalent to a stored or received value. The aforementioned cover claims 29 and 30.

25. As per claim 33, it is an apparatus claim corresponding to claim 26 and it does not teach or define above the information claimed in claim 26. Therefore, claim 33 is rejected under Zhang in view of Friedman and Stallings for the same reasons set forth in the rejection of claim 26.

26. Claims 3, 4, and 11-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang in view of Friedman, and further in view of Schneier Applied Cryptography 2nd Edition (hereinafter Schneier). As per claim 3, Zhang covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Zhang discloses scrambling s and d to create value u (see Zhang, col. 22, lines 31-36), but Zhang does not expressly disclose an encryption function with a symmetric key as the scrambling operation. However as taught by Schneier, scrambling techniques, such as diffusion and confusion, are commonly executed by symmetric encryption algorithms (see Schneier, page 237, 'Confusion and Diffusion'; pages 270-278, Section 12.2 'Description of DES', especially 'Expansion Permutation' and 'S-Box Substitution'). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Schneier to the method of Zhang. Motivation for such an implementation would utilize a standard encryption scheme to scramble s and d to create u.

27. As per claim 4, Zhang covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Zhang does not expressly disclose calculating X(M) by applying both the one-way function H and an encryption function D of a symmetric key to the values u and M. However, as known in the art, encryption steps using symmetric keys are efficient means to hide sensitive values (see Schneier, page 4, 'Symmetric Algorithms'). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Schneier to the invention covered by

Zhang. Motivation for such an implementation would ensure that the processed value is secured.

28. As per claims 11-17, Zhang covers a proving device as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, the processing steps by the proving device as listed in dependent claims 11-17 are generic implementations of well-established cryptosystems as taught by Schneier. In summary, claims 11 and 12 are processing means to implement any type of verification scheme using a challenge variable such as a DSA signature algorithm (see Schneier, pages 486-487, 'Description of DSA', where H(m) is the challenge variable); claims 13-14 are processing means to implement authentication schemes having commitment values such as the Schnorr authentication (see Schneier, page 511, 'Authentication Protocol', where x is the commitment); claims 15 and 17, read on encryption schemes using multiplication, power operations, and modular arithmetic, including DSA signature and Schnorr authentication schemes as listed earlier; and finally, claim 16 reads on operations using elliptic curve cryptosystems (see Schneier, page 480, Section 19.8). It would be obvious to one of ordinary skill in the art at the time the invention was made to perform the processing based on standard cryptosystems. Motivation for such implementations ensures that the proving device is derived from proven cryptosystems.

29. Claims 31-32 and 34-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang in view of Friedman, Schneier, and Stallings. As per claims

31 and 32, Zhang covers an access ticket issuing device as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Although Zhang does not expressly disclose combining two values as defined in claims 31 and 32, this type of operation on two variables is typical especially when the two values are of differing sizes. An example of this strategy is found in DES. A plaintext p is broken into 64-bit segments (p1, p2, ..., pn) and each segment is operated on by a 56 bit key k (see Schneier, pages 270-278, Section 12.2, 'Description of DES'). Furthermore, the resulting value has a standard size corresponding to the number of segments and the processed segment length, which is essential so that resulting values can be reconfigured into alternative but consistent formats. It would be obvious to one of ordinary skill in the art at the time the invention was made to combine two values by segmenting one value and applying each segmented value to the other value. Motivation for such an implementation enables two different formatted values to be combined where each part of the resulting value is dependent on both of the two values.

30. As per claims 34-38, Zhang covers an authentication device as outlined above in the claim 33 rejection under 35 U.S.C. 103(a). Although Zhang does not expressly disclose using the access ticket to update values used in authentication, these steps are obvious implementations for the following reasons: an access ticket expressed as a difference or a quotient of private key x and value X(M) are obvious constructions to show equality/inequality of two values as argued above in the claim 29 and 30 rejections, and further, the updates in claims 34-38 are obvious means to communicate

the resulting discrepancy between x and X(M) to an authenticator in the authentication schemes as summarized by Schneier and listed above. As defined in the applicant's Specification (see expressions 65, 67, and 69 on page 48), the update procedure is defined by applying the following types of operations: z = z + z*(x – X(M)), z = z^(x/X(M)), or z = z/(x/X(M)), wherein the z variable is a challenge or response value defined in a step of a conventional authentication scheme. In these cases, z remains the same if x == X(M), and is updated to a different value if x!= X(M). Furthermore, as taught by Stallings, challenge or response approaches used in authentication methods typically comprise steps of submitting a value by a sender wherein the receiver is required to return the same value back to the sender (see Stallings, page 304, bullet 'Challenge/response'). Hence, the steps of claims 34-38 are simple variations of this theme. It would be obvious to one of ordinary skill in the art at the time the invention was made to update challenge or response values in step(s) of implemented authentication schemes to determine if a generated value is equivalent to a stored or received value and thus determine authentication. Motivation for such an implementation would use simple update functions to determine if authentication has succeeded or failed. The aforementioned cover claims 34-38.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chaum U.S. Patent No. 4,926,480.

Chaum U.S. Patent No. 4,947,430.

Matyas et al. U.S. Patent No. 5,200,999.

Matyas et al. U.S. Patent No. 5,201,000.

Schweiter et al. U.S. Patent No. 5,850,450.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
February 5, 2004

Gilberto B

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100